PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-149337
(43)Date of publication of application : 02.06.1998

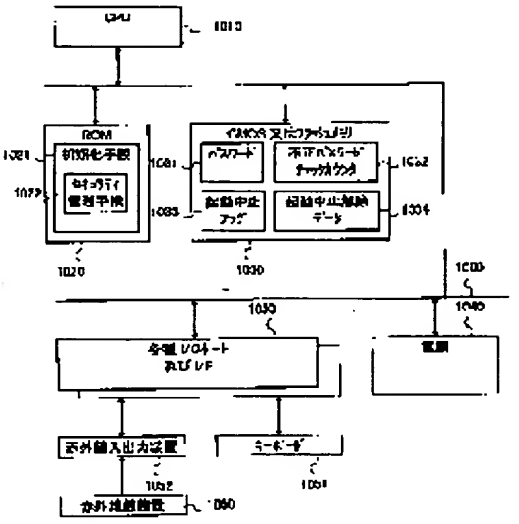
(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 12/14

(21)Application number : 08-309015
(22)Date of filing : 20.11.1996

(71)Applicant : HITACHI LTD
(72)Inventor : FURUKAWA HIROSHI
OTE ICHIRO
KOBAYASHI YUICHI

(54) SECURITY FUNCTION USED FOR START OF SMALL SIZED INFORMATION DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the information, etc., from leaking out to the outsiders by limiting the input frequency of the password that attains a security function in a start mode and stopping semipermanently the start processing if the wrong input operations are performed in times more than a fixed number.
SOLUTION: In regard to a security management means 1022, a CMOS or a flash memory 1030 includes a wrong password check counter 1032 which counts the times of wrong passwords, a start stop flag 1033, a start stop cancel data area 1034 which decides a regular owner when the contents of the flag 1033 are changed to an OFF state from an ON state, and an infrared key device 1060. The flag 1033 is referred to as the first processing of the means 1022, and an interruption occurs in a normal PC start mode as long as the flag value is kept in an ON state. Then the start processing is stopped unless the signal inputted from an I/O port is coincident with the value of the area 1034 which is previously registered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－149337

(43)公開日　平成10年(1998)６月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０		1/00	３７０Ｅ
	12/14	３２０		12/14	３２０Ｃ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平8－309015

(22)出願日　平成８年(1996)11月20日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　古川　博
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　大手　一郎
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　小林　祐一
神奈川県海老名市下今泉810番地株式会社日立製作所オフィスシステム事業部内

(74)代理人　弁理士　小川　勝男

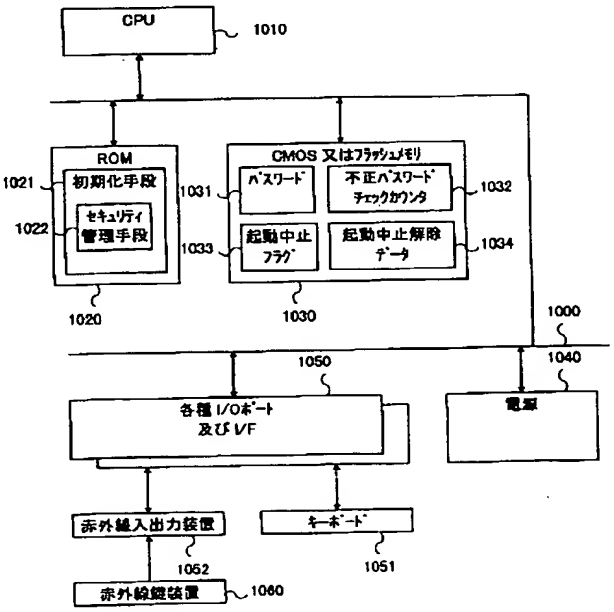
(54)【発明の名称】　小型情報機器の起動時におけるセキュリティ機能

(57)【要約】

【課題】従来の小型情報機器起動時のセキュリティ機能で、パスワードのみのセキュリティ機能では、不正なユーザが小型情報機器の電源を入れ直しさえすれば、何度でもパスワードを入力でき、そのうちパスワードを見破られてしまう危険が存在した。

【解決手段】パスワード入力の回数を制限し、回数を超した場合に小型情報機器そのものの起動を特定の入力信号が入らない限り永遠に中止する機能と、あらかじめ登録した小型情報機器固有でかつ小型情報機器とは別ハードウェア媒体による入力信号によって起動不可状態の小型情報機器の解放を行う機能により実現する。

図１



1

【特許請求の範囲】

【請求項１】小型情報機器で、その起動時にセキュリティ機能を実現するパスワード入力の回数を制限し、一定回数以上の不正な入力が行われた場合に、起動処理そのものを半永久的に中止することを特徴とする小型情報機器起動時におけるセキュリティ機能。

【請求項２】請求項１において、一定回数以上の不正な入力が行われた場合に、上記小型情報機器の起動中止判定用の情報を格納する領域を、上記小型情報機器内の不揮発性読み書き記憶領域内に持つ小型情報機器起動時におけるセキュリティ機能。

【請求項３】請求項１において、半永久的に起動不可になった上記小型情報機器を、小型情報機器毎に固有でかつ小型情報機器とは別ハードウェア媒体による入力信号で解除する小型情報機器起動時におけるセキュリティ機能。

【請求項４】請求項３において、入力された信号の正誤を判定するため、あらかじめ上記ハードウェア媒体の信号を記憶する領域を、上記小型情報機器内の不揮発性読み書き記憶領域内に持つ小型情報機器起動時におけるセキュリティ機能。

【請求項５】請求項１または３において、上記小型情報機器の盗難、紛失時に第三者への小型情報機器内の情報漏洩を防止する小型情報機器起動時におけるセキュリティ機能。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は小型情報機器の起動時のセキュリティ機能に属する。

【０００２】

【従来の技術】従来の小型情報機器起動時のセキュリティ機能では、不揮発性読み書き記憶領域内にあらかじめ登録されたパスワードと同じパスワードを入力した者にしか小型情報機器のアクセスを許可しない機能や、起動処理毎で不正パスワードの入力が一定回数以上の場合、起動処理を中止したり、更にセキュリティレベルの高いパスワードが入力されなければ起動処理が中止される機能は存在した。

【０００３】しかし、このようなパスワードのみのセキュリティ機能では、不正なユーザが小型情報機器の電源を入れ直しさえすれば、何度でもパスワードを入力でき、そのうちパスワードを見破られてしまう危険が存在した。

【０００４】

【発明が解決しようとする課題】本発明では小型情報機器が盗難や紛失等にあった場合に、所有者以外の不正な使用者のアクセスを防ぐセキュリティ機能を小型情報機器の起動時に行い、第三者に小型情報機器の情報等が漏洩することを防ぐ。

【０００５】具体的にはパスワード入力の回数を制限し、回数を超した場合に小型情報機器そのものの起動を特定の入力信号が入らない限り永遠に中止する機能と、あらかじめ登録した小型情報機器固有でかつ小型情報機器とは別ハードウェア媒体による入力信号によって起動不可状態の小型情報機器の解放を行う機能により実現する。

2

【０００６】

【課題を解決するための手段】本発明では、小型情報機器の起動時手段中のセキュリティ管理手段と、起動を中止するための情報を格納する領域と不正パスワードの入力回数記憶する領域を小型情報機器の不揮発性読み書き記憶領域内に有し、これらにより起動時の不正パスワード入力がある一定回数以上行われた場合に小型情報機器の起動そのものを中止する。

【０００７】また、小型情報機器の起動時手段中のセキュリティ管理手段と、小型情報機器とは別ハードウェア媒体と、前記別ハードウェア媒体の入力信号の正誤を判定するためのデータを記憶するための領域を不揮発性読み書き記憶領域内に有し、起動不可状態の小型情報機器を小型情報機器固有でかつ小型情報機器とは別ハードウェア媒体からの入力信号により解放する。

【０００８】

【発明の実施の形態】図面を利用して本発明の一つの実施例を説明する。

【０００９】図１は本発明の前提となる小型情報機器内部の構成の一部を示したものである。ここでは小型情報機器の一例としてパーソナルコンピュータ(以下PCと呼ぶ)を元に話を進める。1000はPC内各装置を結ぶ経路であるバスである。1000のバスには中央演算装置CPU1010、不揮発性読み込み専用記憶領域ROM1020、バックアップ電池等を利用してPC電源オフ時にもデータ値を保持可能な不揮発性読み書き記憶領域CMOSまたはフラッシュメモリ1030、電源装置1040、各種インプット/アウトプットI/O用ポートやインタフェースI/F装置1050等が接続されており、通常前記各装置を使用して演算命令処理を行う。

【００１０】図１において、PCの起動時の処理は以下のように行われる。電源装置1030から電源が供給されると、CPU1010が起動命令を発行し、ROM1020上のPCの初期化処理を行う初期化手段1021が起動する。次に初期化手段1021により、バス1000に接続された各装置の初期化等を行い、キーボード1051や赤外線入出力装置1061等が使用可能な状態になる。

【００１１】現在のPCでは、CMOSまたはフラッシュメモリ1030内にユーザがあらかじめ登録したパスワード1031をチェックし、キーボード1051からパスワードと同じパスワードを入力した者にしかPCをアクセスさせないようにする、初期化手段1021内にセキュリティ管理手段1022をそなえたものが多い。

【００１２】起動時の初期化手段1021内のセキュリティ

管理手段1022による処理の流れを表したものが図２である。2010で電源オンによりPC起動処理が開始されると、2020でCPU1010が起動し起動命令を発効する。2030で命令によりROM1020上の初期化手段1021が起動し、2040で各種I/Oポート及びI/F1050の１つであるキーボードコントローラを有効化し、キーボード1051からの入力を受け付ける状態にする。2050でCMOSまたはフラッシュメモリ1030内に設定されているパスワード情報1031を取得し、2060でユーザに起動時のパスワード入力を求める。2070で2060ユーザが入力したパスワードを判定し、パスワードが2050で取得したパスワードと一致していれば2080に処理が進み、不一致ならば再度起動時のパスワード入力を求めるため2060に戻る。2080ではその他の起動時処理を行い、2090でPCの起動処理が終了する。

【００１３】ここで、図２ようなパスワード機能のみのセキュリティのセキュリティ管理手段1022ではユーザは何度もパスワードを繰り返し入力し、そのPCのパスワードを最後には見つけだしてしまう可能性があった。

【００１４】本発明の特徴は、セキュリティ管理手段1022として、図１のCMOSまたはフラッシュメモリ1030内に、不正パスワードの回数を数える不正パスワードチェックカウンタ1032、起動中止フラグ1033、起動中止フラグ1033の内容をオンからオフに変更する際に正規の所有者であるかを判定するための起動中止解除データ領域10334を持つことと、赤外線鍵装置1060を備えることである。

【００１５】起動中止フラグ1033は、PC起動時の初期化手段1021内のセキュリティ管理手段1022の最初の処理として参照され、もしフラグ値がオン状態であれば通常のPC起動処理に割り込みが入り、あるI/Oポートから、各PC固有でかつPCとは別ハードウェア媒体からの入力信号が入り、それがあらかじめ登録しておいた起動中止解除データ領域1034の値と一致しない限り、起動処理を中止するものである。つまり、この各PC固有でかつPCとは別ハードウェア媒体は鍵のような役目をする。

【００１６】またPC起動時の初期化手段1021内のセキュリティ管理手段1022のパスワード入力で、不正なパスワードを連続して入れると不正パスワードチェックカウンタ1032が加算されていき、ある一定回数以上になると、起動中止フラグ1033は値がオン状態にセットされる。一方、このフラグ値をオフ状態に解除するには、に示したようにあるI/Oポートから、各PC固有でかつPCとは別ハードウェアからの入力信号を入れ、入力された信号がデータ領域1034の値と一致していれば解除されるものとする。

【００１７】本実施例では、各PC固有でかつPCとは別ハードウェア媒体からの入力信号を発信するものとして、赤外線データを発信する赤外線鍵装置1060を使い、最近のPCに標準装備されることが増えてきた赤外線入出力装置1052を通してデータを取得するように説明を行う。な

お赤外線鍵装置1060は、ある決められた一定の間隔でデータを送信する等の独自ハードウェア機構を有し、他の赤外線装置からの信号が赤外線鍵装置1060と同じデータ値を発信しようと、セキュリティ管理手段1022で正規のデータとして受け付けられないようにしてある。

【００１８】この赤外線鍵装置と同じような効果は、ICカード、フロッピーディスクなどの可搬記録媒体等でも可能である。

【００１９】本発明のセキュリティ管理手段1022が、PC起動時の初期化手段1021としてどのような処理の流れになるかを図３、図４を使って示す。2010から2030までは図２で示した従来の処理と変わらない。3010でCMOSまたはフラッシュメモリ1030上の起動中止フラグ1033を取得する。3020で3010で取得した起動中止フラグの状態を判定する。起動中止フラグがオフならば、3030でCMOSまたはフラッシュメモリ1030上の不正パスワードチェックカウンタ1032を0に初期化し、2040に進。逆にオンならば4010に進む。2040から2070も図２で示した従来の処理と同様である。2070でユーザが入力したパスワードとCMOSまたはフラッシュメモリ1030上に設定されているパスワード1031を比較するが一致した場合は、図２で示した従来の処理と同じく2080、2090と処理は続く。逆に一致しなかった場合、3040でCMOSまたはフラッシュメモリ1030上の不正パスワードチェックカウンタ1032をカウントアップし、3040の値を元に3050でユーザが不正パスワードを入力した回数の判定を行い、規定回数に達していなければ、ユーザに再度パスワードを入力することを要求する。一方規定回数に達していれば、3060で起動中止フラグ1033をオンにし、3070で赤外線以外からの入力を行えなくするため、赤外線以外のコントローラを無効化し、4010の赤外線データ入力処理に移行する。そして赤外線データ入力処理を抜けてきた場合、3080で起動中止フラグ1033をオフに初期化し、3020の判定前に戻る。

【００２０】4010の赤外線データ入力処理は、赤外線の入力を有効にするため4020で赤外線ポートを有効化する。続いて4030でCMOSまたはフラッシュメモリ1030上のあらかじめ登録されている各PCに固有な起動中止解除データ1034を取得し、4040で赤外線ポート入力待ち状態になる。4050でユーザが各PCに固有な赤外線鍵1060で赤外線データを赤外線ポートに入力すると、4060で入力された赤外線データが4050で取得したデータと一致するかどうか、更に赤外線鍵のデータが有効かどうかを確認し、一致しなければずっと入力を待つことになる。一致した場合は4070で赤外線データ入力処理を終了することになる。もし、赤外線データ入力待ち段階4040でPCの電源が切られたとしても、次回起動時には起動中止フラグはオン状態であり、常に図４の処理で各PCに固有な鍵のような赤外線データ発信装置から赤外線データが入力されない限り永遠にPCは起動できないことになる。

【００２１】

【発明の効果】本発明は特に可搬可能な小型情報機器等に活用した場合に効果を発生する。

【００２２】例えば可搬な小型情報機器を出張等で出先に持って行き、そこで紛失や盗難にあった場合、従来のパスワードによるセキュリティのみでは、電源をオン/オフを繰り返すことで初期化されるため、何度でもパスワードを入力可能で、そのうちパスワードを見破られ、情報そのものが漏洩する可能性を秘めていた。

【００２３】しかし本発明によれば、ある一定回数のパスワード入力の不正があれば、その後小型情報機器の起動は常に中止されるモードに入る。状態から抜けるには正規所有者等が登録した、小型情報機器単位で固有でかつ小型情報機器とは別ハードウェア媒体による入力信号が必要であり、媒体そのものが盗難等に会わない限り、小型情報機器起動のセキュリティは半永久的に守られる。

【図面の簡単な説明】

【図１】小型情報機器の内部構成のブロック図。

【図２】従来のBIOS起動時処理のセキュリティ機能のフローチャート。

【図３】本発明のBIOS起動時処理のセキュリティ機能のフローチャート。

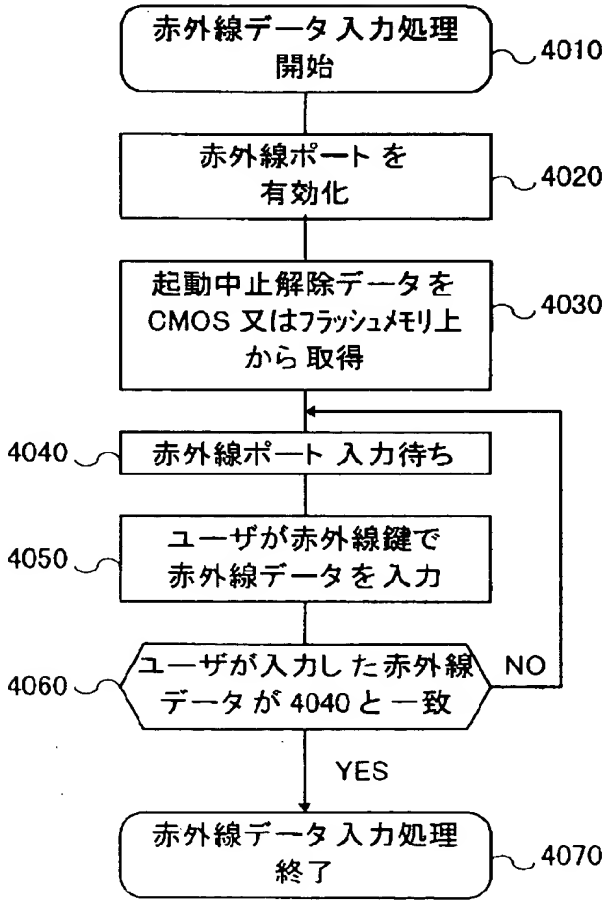
【図４】本発明のBIOS起動時処理のセキュリティ機能のフローチャート。

【符号の説明】

1000…バス、
1010…CPU、
1020…ROM、
1021…BIOS、
1030…CMOSまたはフラッシュメモリ、
1031…パスワード領域、
1032…起動中止フラグ、
1033…データ領域、
1040…電源、
1050…キーボード・マウスコントローラ、
1051…キーボード、
1060…各種I/Oポートおよび I/F、
1061…赤外線入出力装置。

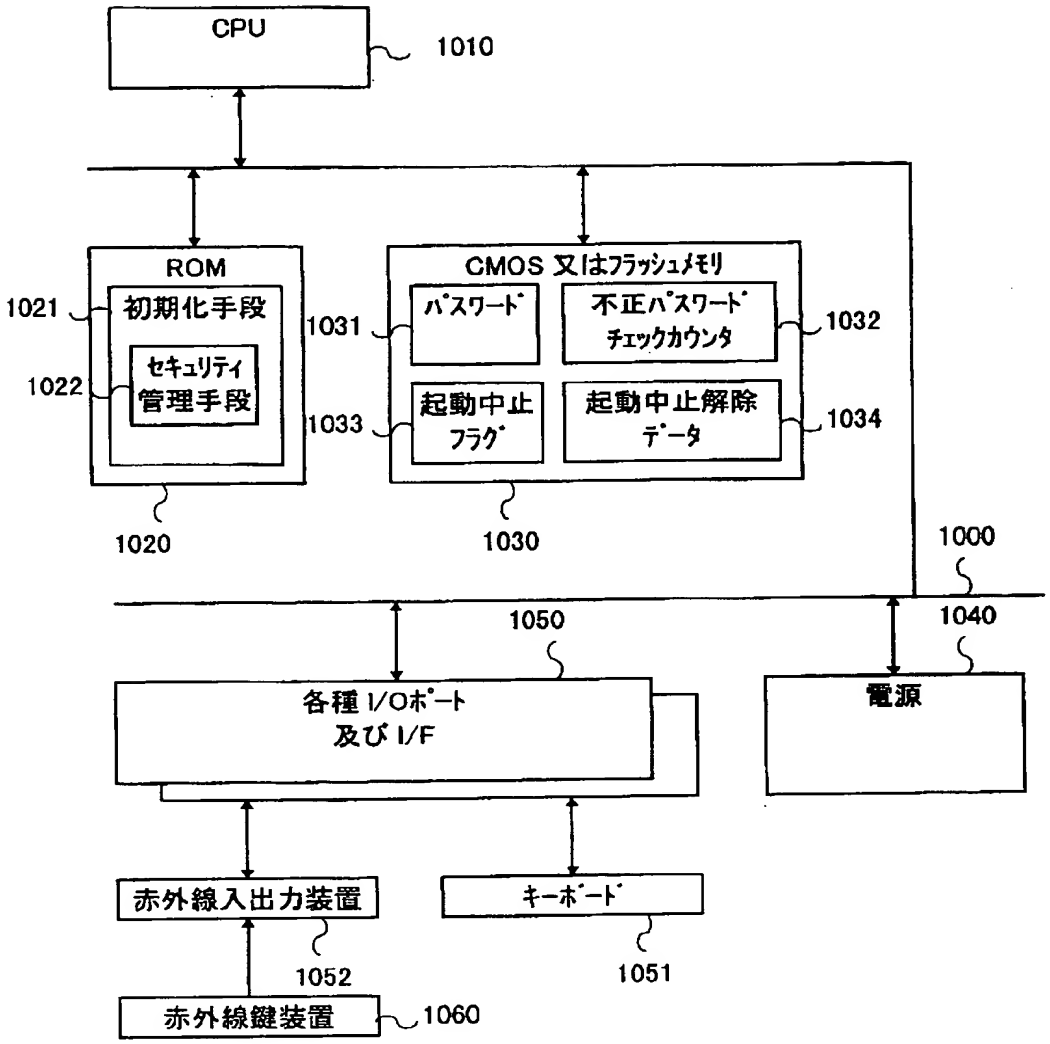
【図４】

図４



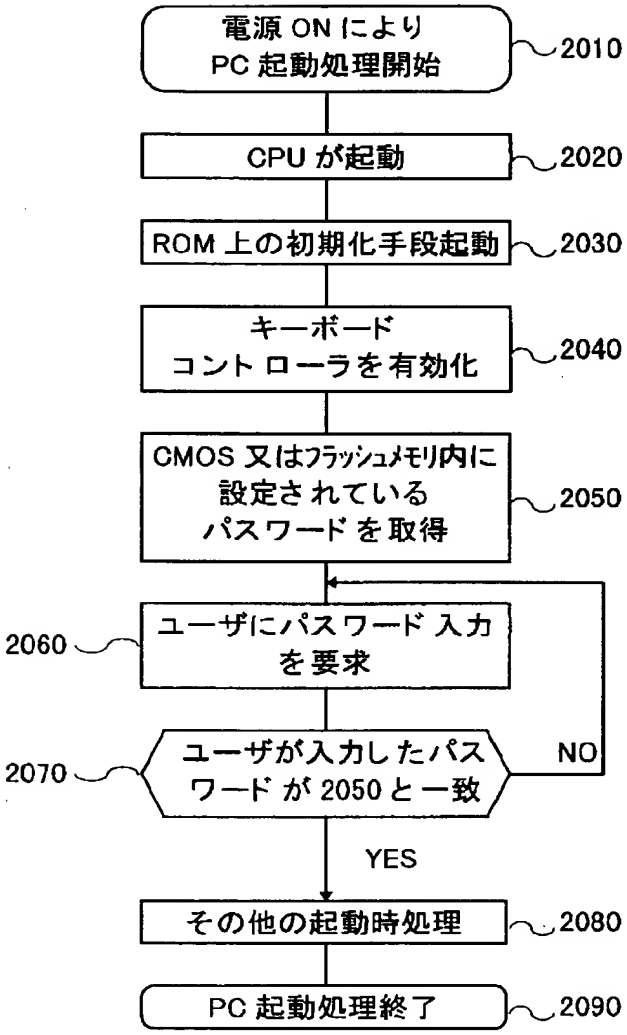
【図１】

図１


CPU
1010
ROM
1021
初期化手段
1022
セキュリティ
管理手段
1020
CMOS 又はフラッシュメモリ
1031
パスワード
1032
不正パスワード
チェックカウンタ
1033
起動中止
フラグ
1034
起動中止解除
データ
1030
1000
1050
1040
各種 I/Oポート
及び I/F
電源
赤外線入出力装置
1052
キーボード
1051
赤外線鍵装置
1060

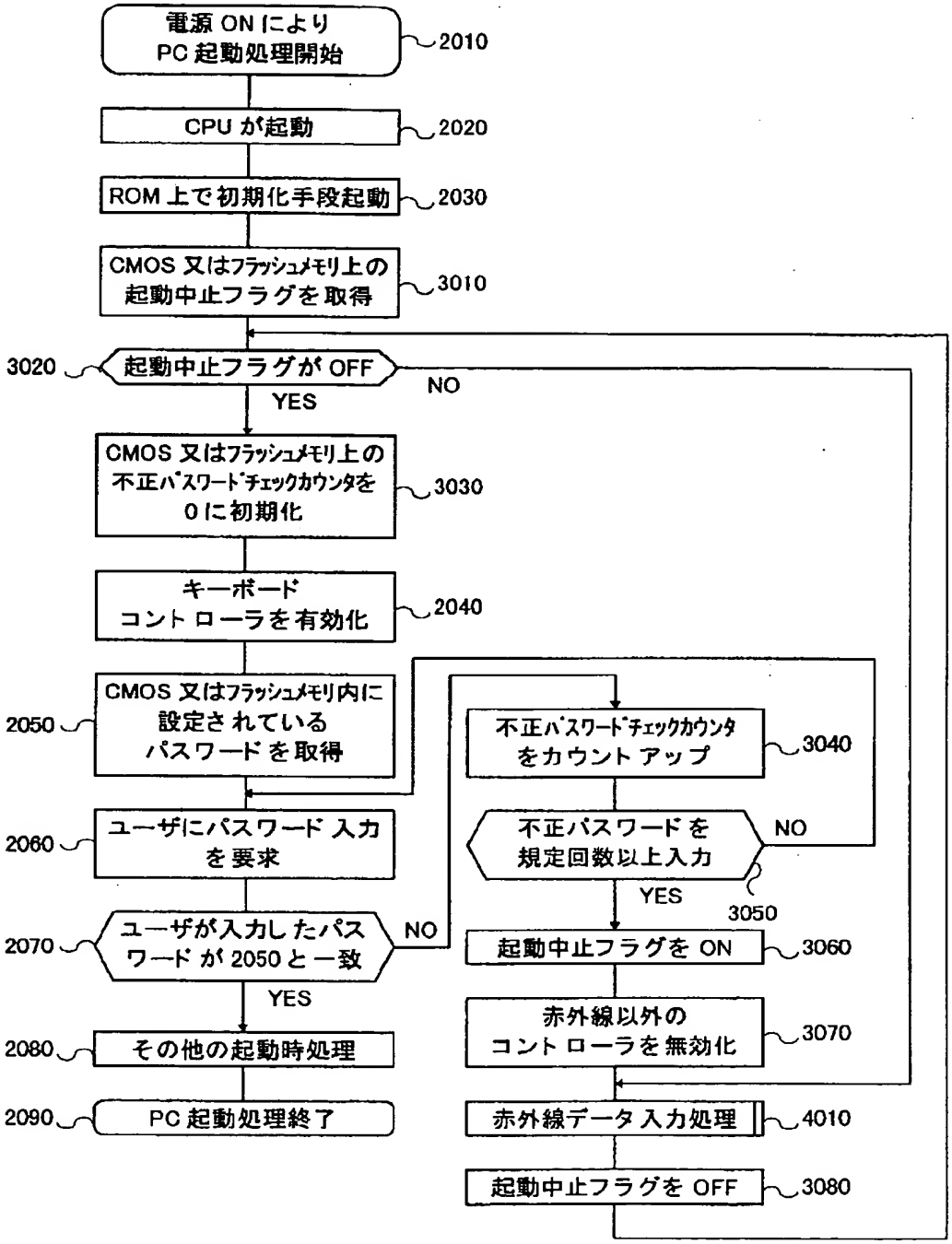
【図２】

図２


電源 ON により
PC 起動処理開始
2010
CPU が起動
2020
ROM 上の初期化手段起動
2030
キーボード
コントローラを有効化
2040
CMOS 又はフラッシュメモリ内に
設定されている
パスワードを取得
2050
2060
ユーザにパスワード入力
を要求
2070
ユーザが入力したパス
ワードが 2050 と一致
NO
YES
その他の起動時処理
2080
PC 起動処理終了
2090

【図３】

図３


電源 ON により PC 起動処理開始
2010
CPU が起動
2020
ROM 上で初期化手段起動
2030
CMOS 又はﾌﾗｯｼｭﾒﾓﾘ上の起動中止フラグを取得
3010
3020
起動中止フラグが OFF
NO
YES
CMOS 又はﾌﾗｯｼｭﾒﾓﾘ上の不正ﾊﾟｽﾜｰﾄﾞﾁｪｯｸｶｳﾝﾀを 0 に初期化
3030
キーボードコントローラを有効化
2040
2050
CMOS 又はﾌﾗｯｼｭﾒﾓﾘ内に設定されているパスワードを取得
2060
ユーザにパスワード入力を要求
2070
ユーザが入力したパスワードが 2050 と一致
NO
YES
2080
その他の起動時処理
2090
PC 起動処理終了
不正ﾊﾟｽﾜｰﾄﾞﾁｪｯｸｶｳﾝﾀをカウントアップ
3040
不正パスワードを規定回数以上入力
NO
YES
3050
起動中止フラグを ON
3060
赤外線以外のコントローラを無効化
3070
赤外線データ入力処理
4010
起動中止フラグを OFF
3080